

EXHIBIT A

FOR PUBLICATION

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

PATRICK CALHOUN; ELAINE
CRESPO; MICHAEL HENRY;
CORNICE WILSON; RODNEY
JOHNSON; CLAUDIA KINDLER,

Plaintiffs-Appellants,

v.

GOOGLE, LLC,

Defendant-Appellee.

No. 22-16993

D.C. No. 4:20-cv-
05146-YGR

OPINION

Appeal from the United States District Court
for the Northern District of California
Yvonne Gonzalez Rogers, District Judge, Presiding

Argued and Submitted July 19, 2024
San Francisco, California

Filed August 20, 2024

Before: MILAN D. SMITH, JR., MARK J. BENNETT,
and ANTHONY D. JOHNSTONE, Circuit Judges.

Opinion by Judge Milan D. Smith, Jr.

SUMMARY*

Data Collection

The panel reversed the district court’s summary judgment in favor of Google, LLC, in a class action alleging that the company surreptitiously collected users’ data in violation of various state and federal laws, and remanded for further proceedings.

Plaintiffs are a group of Google Chrome users who chose not to sync their Chrome browsers with their Google accounts while browsing the web. As they allege in their complaint, Plaintiffs believed, based on the terms of Google’s Chrome Privacy Notice, that their choice not to sync Chrome with their Google accounts meant that certain personal information would not be collected and used by Google. The district court held that Google successfully proved that Plaintiffs consented to its data collection.

The panel explained that the district court should have reviewed the terms of Google’s various disclosures and decided whether a reasonable user reading them would think that he or she was consenting to the data collection. By focusing on “browser agnosticism” instead of conducting the reasonable person inquiry, the district court failed to apply the correct standard. Viewed in the light most favorable to Plaintiffs, browser agnosticism is irrelevant because nothing in Google’s disclosures is tied to what other browsers do.

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

Because applying the correct standard reveals disputes of material fact regarding whether “reasonable” users of Google’s product consented to Google’s data collection practices, the panel remanded the issue of consent—assuming a plaintiff class is certified—to the district court for trial.

COUNSEL

Matthew W.H. Wessler (argued), Gupta Wessler LLP, Washington, D.C.; Neil K. Sawhney, Gupta Wessler LLP, San Francisco, California; Jason O. Barnes, Simmons Hanly Conroy, St. Louis, Missouri; Eric S. Johnson and Jennifer M. Paulson, Simmons Hanly Conroy, Alton, Illinois; Thien An Vinh Truong, Simmons Hanly Conroy, New York, New York; Amy E. Keller, Adam J. Levitt, and Adam Prom, DiCello Levitt LLP, Chicago, Illinois; Corban S. Rhodes and David A. Straite, DiCello Levitt LLP, New York, New York; Lesley Weaver, Bleichmar Fonti & Auld LLP, Oakland, California; for Plaintiffs-Appellants.

Andrew H. Schapiro (argued) and Joseph H. Margolies, Quinn Emanuel Urquhart & Sullivan LLP, Chicago, Illinois; Stephen Broome, Quinn Emanuel Urquhart & Sullivan LLP, New York, New York; Diane Doolittle, Quinn Emanuel Urquhart & Sullivan LLP, Redwood Shores, California; Alyssa Olson and Viola Trebicka, Quinn Emanuel Urquhart & Sullivan LLP, Los Angeles, California; Christopher G. Michel, Quinn Emanuel Urquhart & Sullivan LLP, Washington, D.C.; Jeffrey M. Gutkin, Cooley LLP, San Francisco, California; for Defendant-Appellee.

Jeffrey R. White and Sean Domnick, American Association for Justice, Washington, D.C.; Saveena Takhar, Consumer

Attorneys of California, Sacramento, California; for Amici Curiae American Association for Justice and Consumer Attorneys of California.

Kyle D. Highful, Assistant Solicitor General; Bill Davis, Deputy Solicitor General; Lanora C. Pettit, Principal Deputy Solicitor General; Aaron L. Nielson, Solicitor General; Brent Webster, First Assistant Attorney General; Ken Paxton, Attorney General of Texas; Office of the Attorney General, Austin, Texas; Treg R. Taylor, Attorney General of Alaska; Kris Mayes, Attorney General of Arizona; Kathleen Jennings, Attorney General of Delaware; Anne E. Lopez, Attorney General of Hawaii; Theodore E. Rokita, Attorney General of Indiana; Brenna Bird, Attorney General of Iowa; Daniel Cameron, Attorney General of Kentucky; Jeff Landry, Attorney General of Louisiana; Anthony G. Brown, Attorney General of Maryland; Dana Nessel, Attorney General of Michigan; Lynn Fitch, Attorney General of Mississippi; Aaron D. Ford, Attorney General of Nevada; Raul Torrez, Attorney General of New Mexico; Drew H. Wrigley, Attorney General of North Dakota; Dave Yost, Attorney General of Ohio; Marty J. Jackley, Attorney General of South Dakota; Sean D. Reyes, Attorney General of Utah; Jason S. Miyares, Attorney General of Virginia; for Amici Curiae the State of Texas and 18 Other States.

Alan J. Butler, Sara Geoghegan, and Suzanne Bernstein, Electronic Privacy Information Center, Washington, D.C.; for Amicus Curiae Electronic Privacy Information Center.

Cory L. Andrews and John M. Masslon II, Washington Legal Foundation, Washington, D.C.; for Amicus Curiae Washington Legal Foundation.

Stephanie A. Joyce, Potomac Law Group PLLC, Washington, D.C.; for Amicus Curiae The Computer & Communications Industry Association.

OPINION

M. SMITH, Circuit Judge:

Plaintiff-Appellants Patrick Calhoun, Elaine Crespo, Michael Henry, Cornice Wilson, Rodney Johnson, and Claudia Kindler brought this class action lawsuit against Defendant-Appellee Google, LLC, alleging that the company surreptitiously collected users' data in violation of various state and federal laws. The district court granted summary judgment in favor of Google, holding that Google had successfully proven that Plaintiffs consented to its data collection. For the reasons explained below, we reverse and remand.

FACTUAL AND PROCEDURAL BACKGROUND

Plaintiffs are a group of Google Chrome users who “chose not to ‘Sync’ their [Chrome] browsers with their Google accounts while browsing the web from July 27, 2016 to the present.” As they allege in their complaint, Plaintiffs believed that their choice not to sync Chrome with their Google accounts meant that certain “personal information” would not be collected and used by Google. Their belief was based on the terms of Google’s “Chrome Privacy Notice,” which “describes features that are specific to Chrome,” and states in relevant part:

You don't need to provide any personal information to use Chrome, but Chrome has

different modes you can use to change or improve your browsing experience. Privacy practices are different depending on the mode that you're using.

Basic Browser Mode

The basic browser mode stores information locally on your system [. . .]

The personal information that Chrome stores won't be sent to Google unless you choose to store that data in your Google Account by turning on sync . . .

Sign-in and Sync Chrome Modes

You also have the option to use the Chrome browser while signed in to your Google Account, with or without sync enabled.

[. . .]

Sync. When you sign in to the Chrome browser or a Chromebook and enable sync with your Google Account, your personal information is saved in your Google Account on Google's servers so you may access it when you sign in and sync to Chrome on other computers and devices. This personal information will be used and protected in accordance with the Google Privacy Policy. This type of information can include:

- Bookmarks
- Tabs
- Passwords and Autofill information

- Other browser settings, like installed extensions

Sync is only enabled if you choose . . .

How Chrome handles your synced information

When you enable sync with your Google Account, we use your browsing data to improve and personalize your experience within Chrome . . .

You can change this setting on your Account History page or manage your private data whenever you like. If you don't use your Chrome data to personalize your Google experience outside of Chrome, Google will only use your Chrome data after it's anonymized and aggregated with data from other users . . .

Notwithstanding the above statements, Plaintiffs allege that “Google intentionally and unlawfully causes Chrome to record and send users’ personal information to Google regardless of whether a user elects to Sync or even has a Google account.” Specifically, Plaintiffs allege that “Chrome sends the following personal information to Google when a user exchanges communications with any website that includes Google surveillance source code—

again, regardless of whether a user is logged-in to Google Sync or not”:

- a. The user’s unique, persistent cookie¹ identifiers;
- b. The user’s browsing history in the form of the contents of the users’ GET requests² and information relating to the substance, purport, or meaning of the website’s portion of the communication with the user;
- c. In many cases, the contents of the users’ POST³ communications;
- d. The user’s IP address⁴ and User-Agent information about their device; and
- e. The user’s x-client-data identifier.⁵

¹ Cookies are “small text files stored on the user’s device.” *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020).

² “When an individual internet user visits a web page, his or her browser sends a message called a ‘GET request’ to the web page’s server. The GET request serves two purposes: it first tells the website what information is being requested and then instructs the website to send the information back to the user. The GET request also transmits a referer header containing the personally-identifiable URL information.” *Internet Tracking Litig.*, 956 F.3d at 607.

³ “Like a GET request, a POST request is one of ‘[t]he basic commands that Chrome uses to send the users’ side of a communication.’”

⁴ “An ‘IP address’ is a numerical identifier for each computer or network connected to the Internet.” *Internet Tracking Litig.*, 956 F.3d at 596 n.2.

⁵ “The x-client-data header is an identifier that when combined with IP address and user-agent, uniquely identifies every individual download[ed] version of the Chrome browser.”

A. Motion to Dismiss

At the motion to dismiss stage, Google did not deny collecting Plaintiffs' data while using Chrome in an unsynced mode. Instead, it asserted that Plaintiffs consented to this data collection when they agreed to Google's Privacy Policy,⁶ which policy is cross-referenced in the part of the Chrome Privacy Notice discussing "Sign-in and Sync Chrome modes." Google argued that the Policy "disclosed the alleged data collection" per the following terms:

We collect information about the services that you use and how you use them, like when you . . . visit a website that uses our advertising services, or view and interact with our ads and content.

This information includes: . . . device-specific information . . .

When you use our services or view content provided by Google, we automatically collect and store certain information in server logs, [including] details of how you used our service, such as your search queries . . . device event information such as . . . the date and time of your request and referral URL [and] cookies that may uniquely identify your browser or your Google Account.

⁶ The Privacy Policy is incorporated in Google's Terms of Service (TOS), which all Plaintiffs agreed to.

While the district court recognized that consent is a valid legal defense to Plaintiffs' claims, it rejected Google's arguments that it had met its burden to establish the defense.

First, the court noted that Google's General Terms of Service (TOS), which incorporates the Privacy Policy, states that where "these terms conflict with the service-specific additional terms, the additional terms will govern for that service." It further noted that the Privacy Policy directed readers to "additional terms for particular services," and included a hyperlink to the Chrome Privacy Notice. These statements—combined with Google's more specific representation in the Chrome Privacy Notice that "the personal information that Chrome stores won't be sent to Google unless you . . . turn[] on sync"—led the court to conclude that a reasonable user would not think they were consenting to the data collection at issue. The court noted that a reasonable user viewing these disclosures might think "that if he or she used Chrome without sync, his or her personal information would not be sent to Google."

Second, the court rejected Google's argument that the Chrome Privacy Notice was accurate regarding how Google would treat "the personal information that Chrome stores" because "readers would understand that 'the personal information that Chrome stores'" does not include the data collection at issue in this case. The court rejected this argument because the data collection "falls within the definition of personal information under California law, which governs Google's [TOS]," and the terms of Google's own privacy policy.

In sum, the court concluded that "Google cannot show that Plaintiffs expressly consented to Google's collection of data," and that "[t]o the contrary, Google's representations

might have led a reasonable user to believe that Google did not collect his or her personal information when the user was not synced.” It thus denied Google’s motion to dismiss on its consent defense.⁷

B. Motion for Summary Judgment

Google moved for summary judgment. In its summary judgment briefing, Google introduced two additional notices in support of its consent defense: the “Consent Bump Agreement,” which it launched in June 2016, and the “New Account Creation Agreement,” updated in June 2016.

The “Consent Bump Agreement” “is a push down banner that Google showed to account holders either when they visited a ‘Google owned-and-operated property’ while signed into their account or when users signed into their account for the first time after June 2016.” It reads in relevant part:

[W]hen you use[] Google services like Search and YouTube, you generate data—things like what you’ve searched for and videos you’ve watched. You can find and control that data in My Account under the Web & App Activity setting. With this change, this setting may also include browsing data from Chrome and activity from sites and apps that partner with Google, including those that show ads from Google.

⁷ This case was originally assigned to Judge Lucy H. Koh. After the motion to dismiss order was issued, however, Judge Koh was elevated to the Ninth Circuit, and Judge Yvonne Gonzalez Rogers was assigned to adjudicate the case.

The “New Account Creation Agreement” incorporates the Privacy Policy, and states:

When you search for a restaurant on Google Maps or watch a video on YouTube, for example, we process information about that activity—including information like the video you watched, device IDs, IP addresses, cookie data, and location.

We also process the kinds of information described above when you use apps or sites that use Google services like ads, Analytics, and the YouTube video player . . .

We also combine data among our services and across your devices for these purposes.

The district court referred to these agreements, along with the Privacy Policy, collectively, as “Google’s general policies” to distinguish them from the Chrome-specific Privacy Notice.

Assuming that *only* Google’s “general policies” *or* the Chrome Privacy Notice could govern Google’s conduct in this case, the court identified the threshold issue at summary judgment as “which agreement controls the at-issue data collection.” “Plaintiffs contend[ed] that the Chrome Privacy Notice applie[d] because they are Chrome users using the Chrome browser.” “Google . . . argue[d] that because the data collection at issue . . . is ‘browser-agnostic,’ Google’s general policies apply.”

After holding a lengthy evidentiary hearing on the issue, the court found that the collection of data listed in Plaintiffs’ complaint (the “at-issue data” collection) was “browser-

agnostic,” except for the X-client-data-header.⁸ In other words, the court found that the data Plaintiffs complained was improperly collected was “transmitted to Google regardless of the browser used.”

The court then explained the significance of the “browser-agnostic” finding: “Because the Court finds that the at-issue data collected is not specific to Chrome but browser agnostic, the Court also finds that Google’s general policies apply.” “More specifically, the General Privacy Policy, New Account Creation Agreement, and Consent Bump Agreement governs the collection of those categories of information identified by plaintiffs.”

The district court then explained that all Plaintiffs had consented to the general Privacy Policy, and at least some had agreed to the Consent Bump Agreement and the New Account Creation Agreement. Based on the terms of these agreements, the district court explained that “a reasonable person viewing those disclosures would understand that Google maintains the practices of (a) collecting its users’ data when users use Google services or third party sites that use Google’s services and (b) that Google uses the data for advertising purposes.”

Finally, the district court rejected Plaintiffs’ arguments to the contrary. Most notably, the district court held that the Chrome Privacy Notice did “not negate []” Plaintiffs’ consent to the general policies outlined above. The district

⁸ The district court held that “plaintiffs agreed to Google’s use of the X-Client-header data when they agreed to the Chrome Privacy Notice.”

court entered judgment for Google.⁹ Plaintiffs have timely appealed.

JURISDICTION AND STANDARD OF REVIEW

We have jurisdiction pursuant to 28 U.S.C. § 1291. We review de novo the district court's summary judgment order. *2-Bar Ranch Ltd. P'ship v. U.S. Forest Serv.*, 996 F.3d 984, 990 (9th Cir. 2021).

ANALYSIS

At summary judgment, the following causes of action remained: (1) violation of the California Invasion of Privacy Act; (2) intrusion upon seclusion; (3) breach of contract; (4) breach of the implied covenant of good faith and fair dealing; (5) statutory larceny; and (6) violation of California's Unfair Competition Law. The parties do not dispute that consent is a valid defense to these claims, and that the contours of the defense as established in the Restatement (Second) of Torts.¹⁰ and in state law are as follows.

First, consent "can be [express] or implied, but any consent must be actual." *In re Google Inc.*, No. 13-MD-02430-LHK, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013) (citing *United States v. Van Poyck*, 77 F.3d 285, 292 (9th Cir. 1996)); see also *Pinnacle Museum Tower Ass'n v. Pinnacle Mkt. Dev. (US), LLC*, 282 P.3d 1217, 1224 (Cal. 2012) (stating that general principles of contract law include

⁹ The district court denied Plaintiffs' motion for class certification as moot.

¹⁰ California courts are generally guided by the principles outlined in the Restatement (Second) of Torts. See, e.g., *Korea Supply Co. v. Lockheed Martin Corp.*, 63 P.3d 937, 951 (Cal. 2003).

express or implied consent). For consent to be actual, the disclosures must “explicitly notify” users of the conduct at issue. *In re Google Inc.*, 2013 WL 5423918, at *13. Moreover, “[c]onsent is only effective if the person alleging harm consented ‘to the particular conduct, or to substantially the same conduct’ and if the alleged tortfeasor did not exceed the scope of that consent.” *Tsao v. Desert Palace, Inc.*, 698 F.3d 1128, 1149 (9th Cir. 2012) (“To be effective, consent must be . . . to the particular conduct, or substantially the same conduct.”) (quoting Restatement (Second) of Torts § 892A(2)(b) (1979))).

The parties agree that consent is “an affirmative defense for which defendant bears the burden of proof.” *Van Patten v. Vertical Fitness Grp., LLC*, 847 F.3d 1037, 1044 (9th Cir. 2017). In determining consent, courts consider “whether the circumstances, considered as a whole, demonstrate that a reasonable person understood that an action would be carried out so that their acquiescence demonstrates knowing authorization.” *Smith v. Facebook, Inc.*, 745 F. App’x 8, 8 (9th Cir. 2018). *See, e.g., Long v. Provide Com., Inc.*, 200 Cal. Rptr. 3d 117, 125 (Ct. App. 2016) (disagreeing that a “hyperlink was sufficiently conspicuous to ‘put a reasonable user on notice of the Terms of Use’”). If that user could have plausibly understood the disclosures “as *not* disclosing that [the defendant] would engage in particular conduct,” then the disclosures are insufficient to establish consent. *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 789 (N.D. Cal. 2019).

Before the district court, Plaintiffs had argued that they did not consent to Google’s conduct because a reasonable user viewing the disclosures would not have concluded that they unambiguously disclosed the data collection at issue. *See, e.g.,* Plaintiffs’ Opposition to Summary Judgment,

Calhoun v. Google, 5:20-cv-05146, at 5-6 (Jan. 2, 2022). Specifically, Plaintiffs asserted that the explicit statements in the Chrome Privacy Notice would actually give a reasonable user the *opposite* impression regarding Google’s data collection practices. Further, Plaintiffs argued that—to the extent Google relied on the Privacy Policy to argue otherwise—that Policy also contained statements in favor of Plaintiffs’ interpretation, such as: “the activity information we collect may include . . . Chrome browsing history *you’ve synced with your Google Account*,” and “[y]our Chrome browsing history is *only saved to your account if you’ve enabled Chrome synchronization with your Google Account*.”

Google argues that the General Privacy Policy addresses the “at-issue” data, such as IP addresses and cookies, while the Chrome Privacy Notice reference to “personal information” addresses only Sync-enabled data like browsing history, bookmarks, tabs, passwords and autofill information, and other browser settings. But the parties dispute whether a reasonable person would understand, in the context of all of Google’s representations in its privacy policies, what “personal information” means.

Plaintiffs also argue that Google’s Chrome Privacy Notice also makes representations about data collection beyond Sync-enabled data. For example, the Chrome Privacy Notice states that “[y]ou don’t need to provide any personal information to use Chrome” and that “[p]rivacy practices are different depending on the mode you’re using.” It goes on to state that in “Basic browser mode,” information such as passwords and “cookies or data from websites that you visit” are stored locally on a user’s system. The Notice then provides that “[t]he personal information that Chrome stores won’t be sent to Google unless you . . . turn[] on

sync.” Although Google argues that the reference to “personal information” is sufficient to indicate which subset of data the Notice controls, together, these statements could suggest that the “personal information” the Chrome Privacy Notice addresses includes cookies and IP addresses.

Based on these arguments, the district court should have reviewed the terms of the various disclosures and decided whether a reasonable user reading them would think that he or she was consenting to the data collection, which collection Google has not disputed. *See, e.g., In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 602 (9th Cir. 2020) (identifying “the relevant question” as “whether a user would reasonably expect that Facebook would have access to the user’s individual data,” and reviewing the terms of “Facebook’s privacy disclosures” to answer that question).

However, rather than trying to determine how a reasonable user would understand Google’s various privacy policies, the district court held a 7.5-hour evidentiary hearing which included expert testimony about “whether the data-collection at issue [is] . . . browser-agnostic.” The district court thus made the case turn on a technical distinction unfamiliar to most “reasonable user[s].” If “the data collection at-issue [wa]s specific to Chrome,” the court believed, then the Chrome-specific promises in the Chrome Privacy Notice applied. But if it was “browser-agnostic”—if Google collected the same data from non-Chrome browsers—then all that mattered were the company’s generalized statements in the terms of service and Privacy Policy.

Having determined that the data collection was “browser agnostic,” the district court held that Plaintiffs consented to this collection when they agreed to Google’s general privacy

policies, because under the “browser agnostic terms” of those policies, the data collection was disclosed. The district court therefore did not consider the terms of the Chrome Policy Notice in its analysis. To the extent the district court considered those terms at all, it only mentioned them to say they did not “negate” Plaintiffs’ consent.

By focusing on “browser agnosticism” instead of conducting the reasonable person inquiry, the district court failed to apply the correct standard, despite its recitation of it. Viewing this in the light most favorable to Plaintiffs, browser agnosticism is irrelevant because nothing in Google’s disclosures is tied to what other browsers do. And that is because the governing standard is what a “reasonable user” of a service would understand they were consenting to, not what a technical expert would.

To resist this conclusion, Google cites our unpublished decision in *Smith* to argue that the district court did not err. The *Smith* panel held that “[a] reasonable person viewing [Facebook’s] disclosures would understand that Facebook maintains” certain data collection practices based on the terms of its disclosures.¹¹ *Smith*, 745 F. App’x at 8-9. Google argues that the reasoning in *Smith* applies here because “[t]he transmissions at issue in *Smith* were materially indistinguishable from those in this case.”

¹¹ The relevant disclosure in *Smith* stated: “We collect information when you visit or use third-party websites and apps that use our Services . . . This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us,” and “we use all of the information we have about you to show you relevant ads.” *Smith*, 745 F. App’x at 8.

But the panel in *Smith* did not hold that plaintiffs consented to the data collection because it determined that the data collection at issue was “agnostic.” Rather, it held that plaintiffs consented to the data collection because, analyzing the terms of Facebook’s Terms and Policies, “a reasonable person viewing those disclosures would understand” that Facebook engaged in the contested practices. *Id.*

More to the point, *Smith*, and our recent unpublished decision in *Hammerling v. Google, LLC*, No. 22-17024, 2024 WL 937247, at *2 (9th Cir. Mar. 5, 2024)¹² are inapposite, because plaintiffs in those cases had not argued that Facebook or Google had service-specific privacy policies that could reasonably be read to say the opposite of what its general privacy policies disclosed. The panel in *Smith*, for example, specifically explained that Facebook was not bound by the contrary assurances of other websites’ policies because “Facebook’s Terms and Policies make no such assurance, and Facebook is not bound by promises it did not make.” *Smith*, 745 F. App’x at 9. By contrast, and at least in the light most favorable to plaintiffs, Google did make a promise in its Chrome Privacy Policy that it would not collect certain information absent a user’s voluntary decision to sync, so Google may be “bound by [those] promises.” *Id.*

Google’s “affirmative statement that it would not receive information” in its Chrome Privacy Notice puts this case more in line with *Internet Tracking Litigation* than with *Smith* or *Hammerling*. *Internet Tracking Litig.*, 956 F.3d at 603. There, a panel of our court reversed a district court’s

¹² Google filed a 28(j) letter notifying the court about this March 4, 2024 unpublished decision.

decision to dismiss a complaint in which users of Facebook alleged that the social media site continued to collect their data even after they had logged out. *Id.* at 596. The panel began by assessing “whether a user would reasonably expect that Facebook would have access to the user’s individual data after the user logged out of the application.” *Id.* at 602. It did this by reviewing Facebook’s various “privacy disclosures” *id.*, rather than looking at browser agnosticism.

The panel noted that Facebook’s general Data Use Policy stated that Facebook “receive[s] data whenever you visit a game, application or website that uses [Facebook’s services].” *Id.* To the extent the policy mentioned log in/log out, it stated that the data collection could include “the date and time you visit the site; the web address, . . . and, if you are logged in to Facebook, your user ID.” *Id.* (emphasis omitted). The panel also noted that Facebook’s “Help Center” answered the more specific question of data collection at log in/log out: “[i]f you are logged into Facebook, we also see your user ID number and email address. . . . If you log out of Facebook, we will not receive this information about partner websites but you will also not see personalized experiences on these sites.” *Id.* Based on these disclosures—including the applicable Help Center page which “affirmatively stated that logged-out user data would not be collected,”—the panel held that a reasonable user would not necessarily expect that Facebook would have access to the data after logging out of the site. *Id.*

Discussing other cases on this topic, the panel noted: “[t]hat users in those cases explicitly denied consent does not render those cases distinguishable from the instant case, given Facebook’s *affirmative statements* that it would not receive information from third-party websites after users had logged out. Indeed, in those cases, the critical fact was that

the online entity represented to the plaintiffs that their information would not be collected, but then proceeded to collect it anyway.” *Id.* at 603 (discussing *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 129, 151 (3d Cir. 2015) and *In re Nickelodeon Cons. Priv. Litig.*, 827 F.3d 262, 293–94 (3d Cir. 2016)).

Here, Google’s general Privacy Policy broadly states “that Google collects data about users’ “[a]ctivity on third-party sites and apps that use [Google’s] services.”” *Hammerling*, 2024 WL 937247, at *1 (analyzing same Privacy Policy). Like the general policy in Facebook which only briefly discussed the log in/log out distinction, the Privacy Policy here only briefly mentions the sync/non-sync distinction. Like the “Help Center” in Facebook, the Chrome Privacy Notice includes more detail on the distinctions between Chrome browsing modes, and includes an “affirmative statement[] that it would not receive information,” *Internet Tracking Litig.*, 956 F.3d at 603, from users “unless you choose to . . . turn[] on sync.” Thus, when the disclosures are read together and in the light most favorable to Plaintiffs, a reasonable user would not necessarily understand that they were consenting to the data collection at issue. It was the district court’s failure to apply the correct standard that led to the opposite conclusion.

This point is illustrated by the outcome of a related case, *Brown v. Google LLC*, 685 F. Supp. 3d 909, 930 (N.D. Cal. 2023). In *Brown*, the same district court presided over a related class action lawsuit brought by users of Google Chrome’s “incognito” mode. *Id.* at 919. As in this case, plaintiffs alleged that Google surreptitiously collected their data, notwithstanding statements in the same Chrome Privacy Notice (and on the incognito splash screen) that within Incognito mode “Chrome won’t store certain

information.” *Id.* at 930. As in this case, Google asserted that the *Brown* plaintiffs consented to the Privacy Policy, which Policy disclosed the data collection challenged. *Id.* at 926.

But unlike in this case, the district court rejected Google’s “agnosticism” reasoning, instead properly turning to the disclosures at issue and assessing whether a reasonable user reading them might believe they were consenting to certain practices. *Brown*, 685 F. Supp. 3d at 927-28.

Here, Google had a general privacy disclosure yet promoted Chrome by suggesting that certain information would not be sent to Google unless a user turned on sync. Thus, “Google itself created a situation where there is a dispute as to whether users’ consent of Google’s data collection generally is ‘substantially the same’ as their consent to the collection of their [non-synced] data in particular.” *Id.* at 928.

Whether a “reasonable” user of Google’s computer software at issue in this case consented to a particular data collection practice is not to be determined by attributing to that user the skill of an experienced business lawyer or someone who is able to easily ferret through a labyrinth of legal jargon to understand what he or she is consenting to. Instead, a determination of what a “reasonable” user would have understood must take into account the level of sophistication attributable to the general public, which uses Google’s services.

Because applying the correct standard reveals disputes of material fact regarding whether “reasonable” users of Google’s product consented to Google’s data collection practices, the issue of consent—assuming a plaintiff class is certified—is remanded to the district court for trial.

CONCLUSION

For the foregoing reasons, we REVERSE the order of the district court and REMAND this case for further proceedings consistent with this opinion.